

Entanglement's Benefit Survives an Entanglement-Breaking Channel

Zheshen Zhang,* Maria Tengner, Tian Zhong, Franco N. C. Wong, and Jeffrey H. Shapiro
*Research Laboratory of Electronics, Massachusetts Institute of Technology,
 77 Massachusetts Avenue, Cambridge, Massachusetts 02139, USA*
 (Dated: March 22, 2013)

Entanglement is essential to many quantum information applications, but it is easily destroyed by quantum decoherence arising from interaction with the environment. We report the first experimental demonstration of an entanglement-based protocol that is resilient to loss and noise which destroy entanglement. Specifically, despite channel noise 8.3 dB beyond the threshold for entanglement breaking, eavesdropping-immune communication is achieved between Alice and Bob when an entangled source is used, but no such immunity is obtainable when their source is classical. The results prove that entanglement can be utilized beneficially in lossy and noisy situations, i.e., in practical scenarios.

PACS numbers: 03.67.-a, 42.50.Dv, 03.67.Hk

Entanglement is essential to many quantum information applications [1–11], but it is easily destroyed. Quantum illumination (QI) [12–15] is a radically different entanglement-based paradigm for bosonic channels: it thrives on entanglement-breaking loss and noise. For a given transmitter power, an initially entangled state's nonclassical correlation produces a classical state at the output of an entanglement-breaking channel whose correlation can greatly exceed what any classical input of the same power can yield through that channel. This suggests that bosonic entanglement can be utilized advantageously in practical situations where it does not survive.

First proposed to increase the signal-to-noise ratio (SNR) for detecting a weakly-reflecting target in the presence of strong background noise [12–14], quantum illumination was later shown, theoretically, to enable high data-rate classical communication that is immune to passive eavesdropping [15]. In the latter application, Alice and Bob use an entangled-state input for their data transfer. Eve, however, has no access to Alice's retained portion of the entangled state, so her eavesdropping performance is that of a classical-state input. The resulting disparity between Alice and Eve's performance—in bit-error rate (BER) and information received per transmitted bit—guarantees Alice and Bob's communication security. In this Letter we report the first experimental demonstration of QI's passive-eavesdropping immunity. Aside from its relevance to secure communication, our experiment represents the first time that bosonic entanglement has yielded a strong performance benefit over an entanglement-breaking channel. Thus it implies that the use of entanglement should *not* be dismissed for environments in which it will be destroyed. Moreover, unlike the recent experiment [16] reporting the target-detection advantage of photon-pair correlations, our eavesdropping-immune QI protocol *requires* an initial state that is entangled. Also, our communication protocol uses only one pulse to decode a bit, whereas target detection in [16] depends on the accumulation of enough data to accurately

estimate a covariance.

Our QI communication experiment is shown schematically in Fig. 1. Alice prepares maximally-entangled signal and idler beams using a spontaneous parametric down-converter (SPDC), sending the signal to Bob and retaining the idler. Bob encodes his message bits at 500 kbit/s by applying 0 (message bit = 0) or π rad (message bit = 1) phase shifts on the signal he receives from Alice. Bob then intentionally breaks the signal-idler entanglement by passing his modulated signal light through an erbium-doped fiber amplifier (EDFA), whose amplified spontaneous emission (ASE) noise masks his bit stream from Eve. Eve must rely on the joint classical-state light she has tapped from the Alice-to-Bob and Bob-to-Alice channels, while Alice combines her noisy returned light with her retained idler in a joint measurement to decode Bob's bit stream. Consequently, QI makes Alice's cross-correlation signature between her retained and returned light beams far stronger than Eve's corresponding signature for her two tapped beams, even though Alice and Eve's receivers only have classical states at their disposal.

In Fig. 1, Alice's SPDC uses a 20-mm type-0 phase-matched MgO-doped periodically-poled lithium niobate (MgO:PPLN) crystal that is continuous-wave (cw) pumped at 780 nm, producing signal and idler outputs at 1550 nm and 1570 nm. A coarse wavelength division multiplexer (CWDM) separates the signal and idler and bandlimits them to 16 nm ($W \approx 2$ THz). The $T = 2$ μ s bit duration at 500 kbit/s then contains $M = TW \approx 4 \times 10^6$ signal-idler mode pairs per information bit. At ~ 135 mW pump power, the SPDC generates a source brightness of $N_S = 0.001$ signal (and idler) photons per mode on average. Having $N_S \ll 1$ and $MN_S \gg 1$ are essential for QI. The former ensures that Alice gets a much stronger correlation signature than Eve does, and the latter guarantees that Alice receives sufficient photons/bit to achieve a low error probability. We typically operate at pump levels yielding MN_S values of hundreds to thousands.

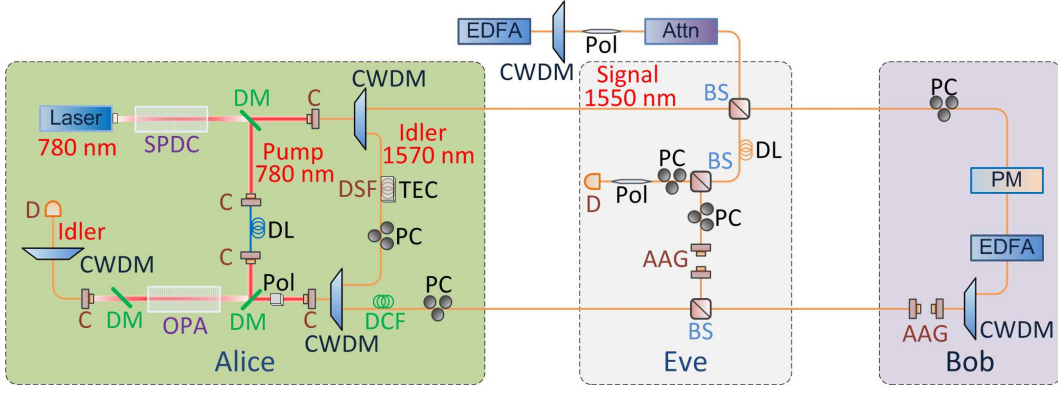


FIG. 1: (color online). Experiment setup. SPDC: spontaneous parametric downconverter; DM: dichroic mirror; C: collimator; CWDM: coarse wavelength-division multiplexer; BS: beam splitter; Attn: attenuator; EDFA: erbium-doped fiber amplifier; DL: delay line; PC: polarization controller; PM: phase modulator; AAG: adjustable air gap; Pol: polarizer; DCF: dispersion-compensating fiber; DSF: dispersion-shifted fiber; TEC: thermoelectric cooler; OPA: optical parametric amplifier; D: detector.

Alice retains the idler in a spool of dispersion-shifted fiber, whose propagation delay matches the Alice-to-Bob-to-Alice delay seen by the signal beam. She sends her signal beam to Bob through a single-mode fiber (SMF) into which Eve has placed a 50-50 beam splitter. Bob applies binary phase-shift keying (BPSK) modulation to the signal light he has received using a phase modulator driven by a pseudorandom bit sequence from a bit-error rate tester (BERT). The modulated light is fed to an EDFA set to a measured gain $G_B \approx 1.34 \times 10^4$ whose ASE noise has per-mode average photon number $N_B \approx 1.46 \times 10^4$. A CWDM filter is used to bandlimit the ASE to the 16 nm occupied by the signal and to attenuate the ASE within the idler spectral band by ~ 30 dB. Complete suppression of the ASE noise outside of the signal band is achieved with a second CWDM in Alice's receiver (and with additional attenuation in Eve's receiver).

Our QI protocol is intrinsically interferometric, so Bob uses a free-space delay line with $\sim 80\%$ efficiency to fine tune the timing between the signal and the idler paths. Dispersion in the SMF's connecting Alice and Bob broadens the SPDC's ~ 0.22 ps biphoton wave-function to ~ 27 ps. Thus Alice injects the light returned from Bob into ~ 10 m of dispersion-compensating fiber before combining it with her retained idler through a CWDM. The signal path sustains a measured channel loss of ~ 16.4 dB that includes SMF coupling loss, fiber-optic component insertion loss, and Eve's 50% (10%) tap placed before (after) Bob's apparatus. (Eve's 50% tap of the Alice-to-Bob channel minimizes her BER when her receiver is ASE limited. However, her removing more than 10% of light from the Bob-to-Alice channel does not improve her BER, because her receiver is ASE limited even with the 10% tap.) Alice's idler suffers ~ 4.1 dB channel loss from SMF coupling and component insertion loss.

Alice decodes Bob's message bits by applying the returned and retained light to the signal and idler ports,

respectively, of a low-gain optical parametric amplifier (OPA), and then doing direct detection on the OPA's idler-port output followed by matched filtering of the output current and threshold-decision logic. In the experiment, the returned and retained light are free-space coupled with the cw pump beam through a dichroic mirror to an OPA based on a 20-mm MgO:PPLN crystal. The OPA converts the cross correlation between the phase-modulated signal and the retained idler into amplitude modulation in the output idler that can be sensed with direct detection. After the OPA, a dichroic mirror is used to remove the pump and the OPA's signal and idler outputs are coupled into an SMF and separated by a CWDM filter. The separated idler is coupled into free space and detected by an avalanche photodiode (APD) setup that is 45% efficient, when coupling and CWDM loss are combined with detector quantum efficiency.

The APD's output current passes through a low-noise current amplifier, whose output is sent to an active high-pass filter, to reject dc, followed by a low-pass filter. The sampled output from the second filter is supplied to a field programmable gate array (FPGA) that yields two outputs. The FPGA program to produce the first output approximates the matched filter for a single bit, and it is subsequently dc shifted and amplified to transistor-transistor logic levels for BER measurements. The second output provides a feedback signal to a lock-in amplifier that is part of a servo-control system (SCS) which stabilizes the relative phases between the OPA pump, Alice's retained idler, and the modulated light she receives from Bob. The SCS also includes a slow thermal-control loop for Alice's fiber spool. Typical incident power at the APD is approximately 10 nW. It is dominated by the signal-band ASE noise converted to the idler band by the OPA. The OPA gain G_A is kept low, $G_A - 1 \ll 1$, to prevent the ASE noise from overwhelming the amplitude modulation in the OPA's idler output. We im-

plement Eve to demonstrate Alice's entangled-input QI performance advantage over what Eve achieves with her classical-state input. Eve decodes Bob's message by combining the light she has tapped from Alice and Bob's transmissions on an asymmetric beam-splitter, and then doing direct detection followed by matched filtering of the output current and threshold-decision logic.

Both Alice and Eve's receivers are sub-optimal, in comparison with minimum error-probability quantum measurements, but both represent their best receivers for which explicit realizations are known. With these receivers Alice and Eve's BERs are given by (see Supplemental Material for details)

$$\text{BER}_A = Q \left(\frac{\sqrt{M}\zeta_A\sqrt{N_S(N_S+1)}}{\sigma_{A+}^{\text{tot}} + \sigma_{A-}^{\text{tot}}} \right) \quad (1)$$

$$\text{BER}_E = Q \left(\frac{\sqrt{M}\zeta_E N_S}{\sigma_{E+}^{\text{tot}} + \sigma_{E-}^{\text{tot}}} \right). \quad (2)$$

Here: Q is the tail integral of the standard Gaussian probability density; $\zeta_A\sqrt{N_S(N_S+1)}$ ($\zeta_E N_S$) is the modulation-depth signature of Bob's message bit seen by Alice (Eve), where ζ_A (ζ_E) is a transmission efficiency; and $\sigma_{A\pm}^{\text{tot}}$ ($\sigma_{E\pm}^{\text{tot}}$) are Alice's (Eve's) per-mode noise standard deviations for bit values 0 and 1. The transmission efficiencies include (see Supplemental Material) the EDFA gain, channel loss, and an effective modulation-depth factor due to residual dispersion and less than optimal mode-pair coupling into an SMF.

The points in Fig. 2 are Alice and Eve's measured BERs. Each point is the average of 10 measurements—1 Msample per measurement, which typically takes only a few seconds—with error bars indicating ± 1 standard deviation. At Alice's maximum SPDC output, Eve's measured modulation depth is insufficient to permit BER_E measurements that would reveal their N_S dependence. Thus to demonstrate that scaling, we replace Alice's SPDC source with the attenuated, CWDM-filtered ASE from an EDFA, as shown in Fig. 1, whose flat-top spectrum thermal state mimics SPDC signal light, but easily produces tens of nW of power for Eve. Eve stores the light split from the Alice-to-Bob channel using a fiber spool, which matches the total fiber length inside Bob's setup, and employs a free-space delay line to fine tune the timing between the two paths. The free-space delay line's coupling is adjusted to optimize Eve's receiver and further suppress the out-of-band ASE noise. Light she has split from the Alice-to-Bob and Bob-to-Alice channels are interfered on a 99-1 beam splitter, with 99% of the power coming from the light taken from the Alice-to-Bob channel, and 1% of the power coming from the light taken from the Bob-to-Alice channel. Eve uses a feedback arrangement similar to Alice's to stabilize her interferometer. Eve obtains her BER values by measuring the combined light using the same APD detection

setup employed by Alice.

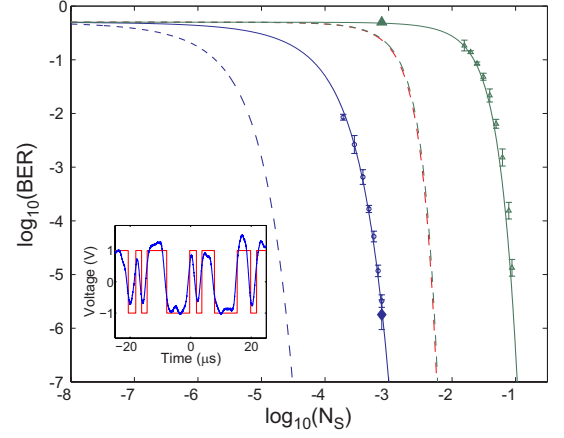


FIG. 2: BER_A and BER_E versus source brightness N_S for 500 kbit/s communication. Inset: 25 bits of OPA-receiver detector output (blue) and Bob's corresponding modulation waveform (red). See text for more information.

The dashed and solid blue curves in Fig. 2 are theory for BER_A when Alice uses a maximally-entangled SPDC and an OPA receiver with gain $G_A - 1 = 1.86 \times 10^{-5}$. The dashed blue curve shows Alice's performance when she has an ideal OPA receiver, viz., no loss of modulation depth due to residual dispersion or sub-optimal mode-pair coupling, unity detection efficiency, unity APD noise figure, no OPA pump-power fluctuations, and no electronics noise; the solid blue curve employs the experimentally-determined values for these receiver nonidealities. The dashed red curve—virtually identical to the dashed green curve—assumes that Alice uses a classical-state source with maximally-correlated signal and idler and an ideal OPA receiver. The gap between the dashed red and solid blue curves shows that Alice's performance using an SPDC source and imperfect OPA reception exceeds what can be achieved with that classical-state source and ideal OPA reception.

The dashed and solid green curves in Fig. 2 are theory for BER_E when Alice uses a maximally-entangled SPDC source or a maximally-correlated classical source and Eve employs an interference receiver. The dashed curve assumes Eve's receiver is ideal; the solid green curve employs the experimentally-determined values for her receiver's nonidealities. The near-identical nature of the dashed red and dashed green curves is a coincidental consequence of our experiment's parameter values.

The blue circles in Fig. 2 are measured BER_A values under the operating conditions used to obtain the solid blue curve; they show our experimental results to be in excellent agreement with theory with no free parameters being adjusted. The filled blue diamond in Fig. 2 is Alice's measured BER at $N_S = 7.81 \times 10^{-4}$ when her OPA gain was increased to $G_A - 1 = 2.48 \times 10^{-5}$, and the filled

green triangle above it is the measured BER_E (Alice’s SPDC is used for this measurement). These two points represent our secure-communication operating point at which $\text{BER}_A = 1.78 \times 10^{-6}$ and $\text{BER}_E \approx 0.5$. The inset provides a visual indication of Alice’s low-BER performance by overlaying 25 bits of her receiver output (blue), with the dc level removed, on Bob’s corresponding modulation waveform (red), which is scaled to match the data’s peak-to-peak range. The joint state of Alice’s returned and retained beams, conditioned on Bob’s BPSK value, is zero-mean and Gaussian. Hence it becomes classical (see Supplemental Material) when $N_B \geq N_B^{\text{thresh}} = 2.14 \times 10^3$, so our measured $N_B = 1.46 \times 10^4$ is 8.3 dB above the threshold for classicality.

The disparity between Alice and Eve’s BERs at the secure-communication operating point, the N_S gap between the dashed red and solid blue theory curves at the same BER values, and N_B ’s exceeding N_B^{thresh} by 8.3 dB confirm the essential feature of quantum illumination that is exploited here in a communication setting: a large performance gap between an entangled-state input and a classical-state input in a lossy and noisy channel.

The open green triangles in Fig. 2 were obtained using attenuated ASE from an EDFA source in lieu of light from a downconverter. They show our measurements to be in excellent agreement with theory with no free parameters being adjusted. The N_S gap between the blue circles and the green triangles in Fig. 2 at the same BER values quantifies Alice and Bob’s entanglement-derived communication advantage when Alice and Eve both use realistic receivers.

At this point it is instructive to consider what would happen had Alice used a cw laser, instead of an SPDC source, and did homodyne detection on the returned light from Bob. That receiver is ASE limited—and essentially quantum optimal—with an error-exponent that is 3 dB inferior to that of an ideal OPA receiver for the same transmitted power, so it might seem to provide a much easier route to passive eavesdropping immunity. Such, however, is not the case: when Eve taps the Alice-to-Bob and Bob-to-Alice links and uses her own homodyne receiver, it too is ASE limited and its BER is the same as Alice’s. So Alice’s initial broadband signal-idler entanglement is absolutely essential to her obtaining immunity to Eve’s passive eavesdropping, because Eve can then only employ the broadband thermal light she taps from Alice and its modulated version that she captures from Bob.

Our measurements show Alice enjoying five orders-of-magnitude error-probability advantage over Eve—when both use realistic receivers—at the secure-communication operating point. Moreover, if Bob’s bit sequence is equally-likely and statistically independent then: (1) Alice receives very close to one bit of information for each bit that Bob has transmitted; and (2) Eve receives nearly zero information about each of Bob’s bits at this operating point. However, both Alice and Eve’s receivers

are limited more by their technical noise than the ASE-generated noise that sets their ultimate sensitivity: at the secure-communication operating point, Alice’s ASE-generated variance is only 26.7% (25.1%) for 0 rad modulation (π rad modulation) of her total noise variance.

It is useful to evaluate the QI performance gap in a different way: Alice’s information advantage over Eve. The two panels in Fig. 3 display Alice’s Shannon information I_{AB} , an upper bound on Eve’s Holevo information χ_{EB}^{UB} , and a lower bound on Alice’s information advantage $\Delta I_{AB}^{\text{LB}} \equiv I_{AB} - \chi_{EB}^{\text{UB}}$. (See Supplemental Material for details.) In the top panel, Alice’s Shannon information is computed using the error probabilities from the solid blue curve in Fig. 2, while the upper bound on Eve’s Holevo information is the most she could learn about an infinitely long sequence of Bob’s bits from an optimum collective quantum measurement on the light she extracts from the Alice-to-Bob and Bob-to-Alice channels. Here we see that with Alice using her imperfect OPA receiver she can get up to 0.8 bits of information advantage, per Bob’s transmitted bit, over Eve’s optimum collective quantum measurement.

A more convincing demonstration that quantum illumination offers Alice a significant information advantage is shown in the bottom panel of Fig. 3. Here we have changed the beam splitter that Eve uses to tap the Bob-to-Alice transmission to have 10% transmissivity instead of the 90% value used in our experiment. Under these conditions, Eve gets the same amount of Alice’s light that Bob does and nine times the amount of Bob’s light that Alice does. Nevertheless, the upper bound on her Holevo information is unchanged from what is seen in the top panel. This is because her received BPSK modulation depth and the standard deviation of the ASE-generated noise that dominates the fluctuations in the jointly-Gaussian state she receives both increase in proportion to the fraction of the light she taps. Alice’s BER, however, is somewhat degraded by reducing the amount of light she gets from Bob, because of her receiver’s technical noise. Consequently, her information advantage over Eve’s optimum collective quantum measurement now peaks at 0.66 bits/bit.

Our experiment demonstrates the QI-communication protocol’s immunity to *passive* eavesdropping that was predicted, theoretically, in [15]. That reference already noted that this protocol is vulnerable to *active* attacks, in which Eve injects her own light into Bob’s terminal. Indeed, Eve could inject her own SPDC signal light into Bob, retaining her source’s idler light for use with the light she taps from the Bob-to-Alice channel. Steps that could be taken to ward off active attacks were suggested in [15], and initial analyses of many of these approaches have been performed [17], but more work is needed on defeating active attacks.

In conclusion, we have demonstrated that the benefits of bosonic entanglement can be reaped over an

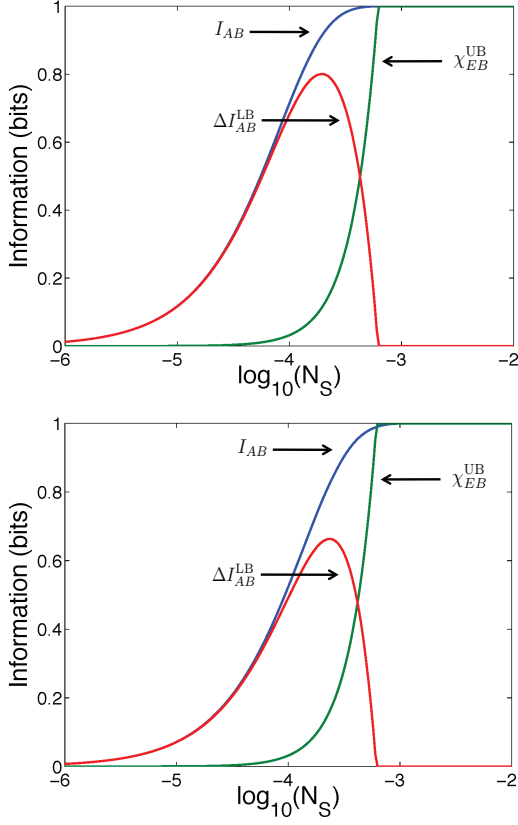


FIG. 3: (color online). Alice’s Shannon information, an upper bound on Eve’s Holevo information, and a lower bound on Alice’s information advantage, versus Alice’s source brightness N_S . The top panel computes Alice’s Shannon information using the error probabilities from the solid blue curve in Fig. 2. The bottom panel computes Alice’s Shannon information when Eve takes 90% of the Bob-to-Alice light instead of the 10% she receives in the top panel.

entanglement-breaking channel. Our QI protocol experimentally achieved more than five orders-of-magnitude BER advantage for Alice over a passive eavesdropping Eve when both use realistic receivers. Furthermore, based on the excellent fit between our data and theory, we claim that Alice enjoys an information advantage that can exceed 0.6 bits per Bob’s transmitted bit over the optimum collective quantum Eve when Eve taps 50% of the Alice’s transmission and 90% of Bob’s transmission. These advantages are consequences of Alice’s initial broadband signal-idler entanglement, because they disappear when Alice’s signal-idler phase-sensitive cross correlation is classical, or when Alice uses a laser source. The meta-lesson of our experiment is as follows: the performance disparity between a QI entangled-state input and a thermal-state input in communication over a lossy, noisy bosonic channel suggests that entanglement may be utilized to good effect in other entanglement-breaking environments.

The authors thank Eric Dauler for the loan of the bit-

error rate tester. This research was supported by an ONR Basic Research Challenge grant.

* Electronic address: zszhang@mit.edu

- [1] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, Phys. Rev. Lett. **70**, 1895 (1993).
- [2] D. Bouwmeester, J.-W. Pan, K. Mattle, M. Eibl, H. Weinfurter, and A. Zeilinger, Nature **390**, 575 (1997).
- [3] X.-S. Ma, T. Herbst, T. Scheidl, D. Wang, S. Kropatschek, W. Naylor, B. Wittmann, A. Mech, J. Kofler, E. Anisimova, V. Makarov, T. Jennewein, R. Ursin, and A. Zeilinger, Nature **489**, 269 (2012).
- [4] H. J. Kimble, Nature **453**, 1023 (1998).
- [5] C. H. Bennett and S. J. Wiesner, Phys. Rev. Lett. **69**, 2881 (1992).
- [6] K. Mattle, H. Weinfurter, P. G. Kwiat, and A. Zeilinger, Phys. Rev. Lett. **76**, 4656 (1996).
- [7] J. T. Barreiro, T.-C. Wei, and P. G. Kwiat, Nature Phys. **4**, 282 (2008).
- [8] P. Shor, SIAM J. Comput. **26**, 1484 (1997).
- [9] L. M. K. Vandersypen, M. Steffen, G. Breyta, C. S. Yannoni, M. H. Sherwood, and I. C. Chuang, Nature **414**, 883 (2001).
- [10] A. Politi, J. C. F. Matthews, and J. L. O’Brien, Science **325**, 1221 (2009).
- [11] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
- [12] S. Lloyd, Science **321**, 1463 (2008).
- [13] S.-H. Tan, B. I. Erkmen, V. Giovannetti, S. Guha, S. Lloyd, L. Maccone, S. Pirandola, and J. H. Shapiro, Phys. Rev. Lett. **101**, 253601 (2008).
- [14] S. Guha, and B. I. Erkmen, Phys. Rev. A **80**, 052310 (2009).
- [15] J. H. Shapiro, Phys. Rev. A **80**, 022320 (2009).
- [16] E. D. Lopaeva, I. Ruo Berchera, I. P. Degiovanni, S. Olivares, G. Brida, and M. Genovese, Phys. Rev. Lett. in press; arXiv1303.4304 [quant-ph].
- [17] W. Xu and J. H. Shapiro, “Defeating active eavesdropping with quantum illumination,” in *Quantum Communication, Measurement and Computing (QCMC): The Tenth International Conference*, AIP Conf. Proc. **1363**, 31–34 (2011).
- [18] S. Pirandola and S. Lloyd, Phys. Rev. A **78**, 012331 (2008).

Supplemental Material

I. THE COMMUNICATION MODEL

Figure 4 shows a conceptual schematic for our experiment. The $\{\hat{a}_{S_i}\}$ and $\{\hat{a}_{I_i}\}$ are signal and idler annihilation operators for one of the M independent, identically-distributed, signal-idler mode pairs produced by Alice's spontaneous parametric downconverter (SPDC). The annihilation operators \hat{a}_I^\pm and \hat{a}_E^\pm are associated with the modes Alice and Eve measure, respectively, from a single signal-idler mode pair, where the \pm superscripts here and elsewhere in the figure represent Bob's ± 1 (0 or π rad) binary phase-shift keying (BPSK) modulation. The transmissivities $\kappa_I, \kappa_A, \kappa_1, \kappa_B, \kappa'_B, \kappa_2, \kappa'_A, \kappa_d, \kappa_E$, and κ'_d model losses—including detector quantum efficiencies—in Alice, Bob, and Eve's terminals and the propagation channels that link them, with the annihilation operators $\{\hat{v}_I, \hat{v}_A, \hat{v}_1, \hat{v}_B, \hat{v}'_B, \hat{v}_2, \hat{v}'_A, \hat{v}_d, \hat{v}_E, \hat{v}'_d\}$ representing vacuum-state auxiliary modes. Bob's erbium-doped fiber amplifier (EDFA) has gain G_B and Alice's optical parametric amplifier (OPA) has gain G_A . Eve chooses the transmissivities κ_E and η_E to minimize her bit error rate (BER). Additional details are as follows.

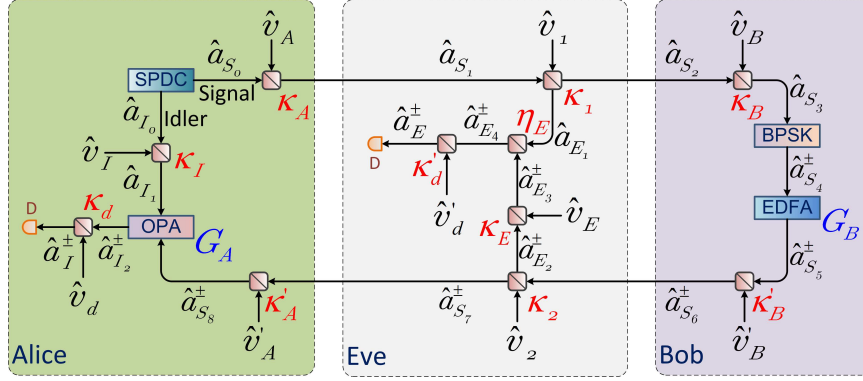


FIG. 4: Conceptual model for secure communication based on quantum illumination. SPDC: spontaneous parametric downconverter. BPSK: binary phase-shift keying. EDFA: erbium-doped fiber amplifier. D: detector. OPA: optical parametric amplifier.

Propagation and detection loss. Propagation and detection loss are accounted for, in Fig. 4, by beam splitters. Each of these is modeled by the annihilation-operator relation

$$\hat{a}_{\text{out}} = \sqrt{\kappa} \hat{a}_{\text{in}} + \sqrt{1 - \kappa} \hat{v}, \quad (3)$$

in terms of the input \hat{a}_{in} , the output \hat{a}_{out} , and a vacuum-state auxiliary mode \hat{v} , where $0 < \kappa < 1$ is the beam-splitter's transmissivity.

BPSK model. Bob's BPSK modulator is modeled, for each signal mode, by the annihilation-operator relation

$$\hat{a}_{S_4}^\pm = \pm \hat{a}_{S_3}, \quad (4)$$

where \pm denotes the common bit value applied to *all* M signal modes.

EDFA theory. Bob's EDFA is modeled, for each signal mode, by the annihilation-operator relation

$$\hat{a}_{S_5}^\pm = \sqrt{G_B} \hat{a}_{S_4}^\pm + \sqrt{G_B - 1} \hat{a}_{SE}^\dagger, \quad (5)$$

in terms of the amplifier's gain G_B and a thermal-state spontaneous-emission mode \hat{a}_{SE} ; the average photon-number per mode of amplified spontaneous emission (ASE) at the amplifier's output is $N_B = (G_B - 1)(\langle \hat{a}_{SE}^\dagger \hat{a}_{SE} \rangle + 1)$.

OPA theory. Alice's OPA is modeled, for each returned-retained mode pair, by the annihilation-operator relation

$$\hat{a}_{I_2}^\pm = \sqrt{G_A} \hat{a}_{I_1} + \sqrt{G_A - 1} \hat{a}_{S_8}^{\pm\dagger}. \quad (6)$$

II. MODE-PAIR PHOTON STATISTICS

A single signal-idler mode pair $\{\hat{a}_{S_0}, \hat{a}_{I_0}\}$ from Alice's continuous-wave spontaneous parametric downconverter is in the maximally-entangled, zero-mean, jointly-Gaussian state $\hat{\rho}_{SI}$ whose density operator is completely characterized by the covariance matrix $\Gamma_{SI} \equiv \langle [\hat{a}_{S_0}^\dagger \hat{a}_{I_0}^\dagger \hat{a}_{S_0} \hat{a}_{I_0}]^T [\hat{a}_{S_0} \hat{a}_{I_0} \hat{a}_{S_0}^\dagger \hat{a}_{I_0}^\dagger] \rangle$ given by

$$\Gamma_{SI} = \begin{bmatrix} N_S & 0 & 0 & \sqrt{N_S(N_S+1)} \\ 0 & N_S & \sqrt{N_S(N_S+1)} & 0 \\ 0 & \sqrt{N_S(N_S+1)} & N_S+1 & 0 \\ \sqrt{N_S(N_S+1)} & 0 & 0 & N_S+1 \end{bmatrix}, \quad (7)$$

where N_S is the source brightness (average number of signal-idler photon pairs per mode). This density operator plus the input-output operator evolutions associated with the beam splitters, phase modulator, and optical amplifiers shown in the quantum illumination conceptual model from Fig. 4 determine Alice and Eve's single-mode photon-counting statistics, namely those of the $\hat{a}_I^{\pm\dagger}\hat{a}_I^\pm$ and $\hat{a}_E^{\pm\dagger}\hat{a}_E^\pm$ operators, respectively. Because all of the preceding evolutions are linear, with the beam splitter's free inputs being in their vacuum states and the EDFA's free input being in a thermal state, it follows that the \hat{a}_I^\pm and \hat{a}_E^\pm modes are in zero-mean Gaussian states. Hence their photon-counting statistics are Bose-Einstein, with variances that satisfy

$$\sigma_{A\pm}^2 = N_A^\pm(N_A^\pm + 1), \quad (8)$$

and

$$\sigma_{E\pm}^2 = N_E^\pm(N_E^\pm + 1), \quad (9)$$

in terms of their average photon numbers $N_A^\pm \equiv \langle \hat{a}_I^{\pm\dagger}\hat{a}_I^\pm \rangle$ and $N_E^\pm \equiv \langle \hat{a}_E^{\pm\dagger}\hat{a}_E^\pm \rangle$. It is now simple to back-propagate along the chain of linear evolutions to obtain explicit results for these average photon numbers.

For Alice, including the effect of imperfect dispersion compensation and allowing for sub-optimal mode-pair coupling, we have that

$$N_A^\pm = \kappa_d \langle \hat{a}_{I_2}^{\pm\dagger}\hat{a}_{I_2}^\pm \rangle \quad (10)$$

$$= \kappa_d \langle (\sqrt{G_A}\hat{a}_{I_1} + \sqrt{G_A-1}\hat{a}_{S_8}^{\pm\dagger})^\dagger (\sqrt{G_A}\hat{a}_{I_1} + \sqrt{G_A-1}\hat{a}_{S_8}^{\pm\dagger}) \rangle \quad (11)$$

$$= \kappa_d G_A \langle \hat{a}_{I_1}^\dagger \hat{a}_{I_1} \rangle + \kappa_d (G_A - 1) + \kappa_d (G_A - 1) \langle \hat{a}_{S_8}^{\pm\dagger}\hat{a}_{S_8}^\pm \rangle \\ \pm 2\eta_d^A \kappa_d \sqrt{G_A(G_A-1)} \text{Re}(\langle \hat{a}_{I_1}\hat{a}_{S_8}^\pm \rangle), \quad (12)$$

where

$$\langle \hat{a}_{I_1}^\dagger \hat{a}_{I_1} \rangle = \kappa_I \langle \hat{a}_{I_0}^\dagger \hat{a}_{I_0} \rangle = \kappa_I N_S, \quad (13)$$

$$\langle \hat{a}_{S_8}^{\pm\dagger}\hat{a}_{S_8}^\pm \rangle = \kappa'_A \kappa_2 \kappa'_B \langle \hat{a}_{S_5}^{\pm\dagger}\hat{a}_{S_5}^\pm \rangle \quad (14)$$

$$= \kappa'_A \kappa_2 \kappa'_B G_B \langle \hat{a}_{S_4}^{\pm\dagger}\hat{a}_{S_4}^\pm \rangle + \kappa'_A \kappa_2 \kappa'_B N_B \quad (15)$$

$$= \kappa'_A \kappa_2 \kappa'_B G_B \kappa_B \kappa_1 \kappa_A \langle \hat{a}_{S_0}^\dagger \hat{a}_{S_0} \rangle + \kappa'_A \kappa_2 \kappa'_B N_B \quad (16)$$

$$= \kappa'_A \kappa_2 \kappa'_B G_B \kappa_B \kappa_1 \kappa_A N_S + \kappa'_A \kappa_2 \kappa'_B N_B, \quad (17)$$

$$\langle \hat{a}_{I_1}\hat{a}_{S_8}^\pm \rangle = \sqrt{\kappa_I \kappa'_A \kappa_2 \kappa'_B} \langle \hat{a}_{I_0}\hat{a}_{S_5}^\pm \rangle \quad (18)$$

$$= \sqrt{\kappa_I \kappa'_A \kappa_2 \kappa'_B G_B} \langle \hat{a}_{I_0}\hat{a}_{S_4}^\pm \rangle \quad (19)$$

$$= \pm \sqrt{\kappa_I \kappa'_A \kappa_2 \kappa'_B G_B \kappa_B \kappa_1 \kappa_A} \langle \hat{a}_{I_0}\hat{a}_{S_0} \rangle \quad (20)$$

$$= \pm \sqrt{\kappa_I \kappa'_A \kappa_2 \kappa'_B G_B \kappa_B \kappa_1 \kappa_A N_S (N_S + 1)}, \quad (21)$$

d_A is her ideal receiver's modulation depth, and η_d^A is its modulation-depth efficiency factor. Combining the preceding results we obtain,

$$N_A^\pm = \kappa_d G_A \kappa_I N_S + \kappa_d (G_A - 1) + \kappa_d (G_A - 1) \kappa'_A \kappa_2 \kappa'_B G_B \kappa_B \kappa_1 \kappa_A N_S + \kappa_d (G_A - 1) \kappa'_A \kappa_2 \kappa'_B N_B \\ \pm 2\eta_d^A \kappa_d \sqrt{G_A (G_A - 1) \kappa_I \kappa'_A \kappa_2 \kappa'_B G_B \kappa_B \kappa_1 \kappa_A N_S (N_S + 1)}, \quad (22)$$

from which it follows that

$$\eta_d^A d_A \equiv N_A^+ - N_A^- = 4\eta_d^A \kappa_d \sqrt{G_A (G_A - 1) \kappa_I \kappa'_A \kappa_2 \kappa'_B G_B \kappa_B \kappa_1 \kappa_A N_S (N_S + 1)}. \quad (23)$$

In the Letter, we have used $\zeta_A \sqrt{N_S (N_S + 1)} \equiv \eta_d^A d_A$.

Similar to what we did in the previous paragraph, we have for Eve that

$$N_E^\pm = \kappa'_d \langle \hat{a}_{E_4}^{\pm\dagger} \hat{a}_{E_4}^\pm \rangle \quad (24)$$

$$= \kappa'_d \langle (\sqrt{\eta_E} \hat{a}_{E_1} + \sqrt{1 - \eta_E} \hat{a}_{E_3}^\pm)^\dagger (\sqrt{\eta_E} \hat{a}_{E_1} + \sqrt{1 - \eta_E} \hat{a}_{E_3}^\pm) \rangle \quad (25)$$

$$= \kappa'_d \eta_E \langle \hat{a}_{E_1}^\dagger \hat{a}_{E_1} \rangle + \kappa'_d (1 - \eta_E) \langle \hat{a}_{E_3}^{\pm\dagger} \hat{a}_{E_3}^\pm \rangle + 2\eta_d^E \kappa'_d \sqrt{\eta_E (1 - \eta_E)} \text{Re}(\langle \hat{a}_{E_1}^\dagger \hat{a}_{E_3}^\pm \rangle) \quad (26)$$

$$= \kappa'_d \eta_E (1 - \kappa_1) \kappa_A \langle \hat{a}_{S_0}^\dagger \hat{a}_{S_0} \rangle + \kappa'_d (1 - \eta_E) \kappa_E (1 - \kappa_2) \kappa'_B \langle \hat{a}_{S_5}^{\pm\dagger} \hat{a}_{S_5}^\pm \rangle \\ + 2\eta_d^E \kappa'_d \sqrt{\eta_E (1 - \eta_E) (1 - \kappa_1) \kappa_A \kappa_E (1 - \kappa_2) \kappa'_B} \text{Re}(\langle \hat{a}_{S_0}^\dagger \hat{a}_{S_5}^\pm \rangle), \quad (27)$$

where

$$\langle \hat{a}_{S_5}^{\pm\dagger} \hat{a}_{S_5}^\pm \rangle = G_B \kappa_B \kappa_1 \kappa_A N_S + N_B, \quad (28)$$

$$\langle \hat{a}_{S_0}^\dagger \hat{a}_{S_5}^\pm \rangle = \pm \sqrt{G_B \kappa_B \kappa_1 \kappa_A N_S^2}, \quad (29)$$

d_E is her ideal receiver's modulation depth, and η_d^E is its modulation-depth efficiency factor. Combining the preceding results we get

$$N_E^\pm = \kappa'_d \eta_E (1 - \kappa_1) \kappa_A N_S + \kappa'_d (1 - \eta_E) \kappa_E (1 - \kappa_2) \kappa'_B G_B \kappa_B \kappa_1 \kappa_A N_S + \kappa'_d (1 - \eta_E) \kappa_E (1 - \kappa_2) \kappa'_B N_B \\ \pm 2\eta_d^E \kappa'_d \sqrt{\eta_E (1 - \eta_E) (1 - \kappa_1) \kappa_A^2 \kappa_E (1 - \kappa_2) \kappa'_B G_B \kappa_B \kappa_1 N_S^2}, \quad (30)$$

from which it follows that

$$\eta_d^E d_E \equiv N_E^+ - N_E^- = 4\eta_d^E \kappa'_d \sqrt{\eta_E (1 - \eta_E) (1 - \kappa_1) \kappa_A^2 \kappa_E (1 - \kappa_2) \kappa'_B G_B \kappa_B \kappa_1 N_S^2}. \quad (31)$$

In the Letter, we have used $\zeta_E N_S \equiv \eta_d^E d_E$.

In order to evaluate our bound, developed below, on Eve's Holevo information, we need expressions for $N_{E_1} \equiv \langle \hat{a}_{E_1}^\dagger \hat{a}_{E_1} \rangle$, $N_{E_3} \equiv \langle \hat{a}_{E_3}^{\pm\dagger} \hat{a}_{E_3}^\pm \rangle$, and $C_{E_1 E_3}^\pm \equiv \langle \hat{a}_{E_1}^\dagger \hat{a}_{E_3}^\pm \rangle$. These are obtained as follows. For N_{E_1} we have that

$$N_{E_1} = (1 - \kappa_1) \kappa_A \langle \hat{a}_{S_0}^\dagger \hat{a}_{S_0} \rangle = (1 - \kappa_1) \kappa_A N_S. \quad (32)$$

For N_{E_3} we have that

$$N_{E_3} = (1 - \kappa_2) \kappa'_B \langle \hat{a}_{S_5}^{\pm\dagger} \hat{a}_{S_5}^\pm \rangle = (1 - \kappa_2) \kappa'_B G_B \kappa_B \kappa_1 \kappa_A N_S + (1 - \kappa_2) \kappa'_B N_B. \quad (33)$$

For $C_{E_1 E_3}^\pm$ we have that

$$C_{E_1 E_3}^\pm = \sqrt{\kappa_A (1 - \kappa_1) (1 - \kappa_2) \kappa'_B} \langle \hat{a}_{S_0}^\dagger \hat{a}_{S_5}^\pm \rangle = \pm \sqrt{\kappa_A^2 (1 - \kappa_1) (1 - \kappa_2) \kappa'_B G_B \kappa_B \kappa_1 N_S^2}. \quad (34)$$

III. ALICE AND EVE'S PER-MODE NOISE VARIANCES

The per-mode conditional variances for Alice and Eve's ideal receivers when Bob's BSPK modulation is 0 rad (+) or π rad (−) are the Bose-Einstein variances $\sigma_{A\pm}^2$ and $\sigma_{E\pm}^2$, respectively. However, Alice and Eve's avalanche photodiodes have noise figure F_{APD} , their detection systems have electronics noise with per-mode variance σ_D^2 , and Alice's OPA receiver has a per-mode conditional variance $\sigma_{P\pm}^2 = 0.2\sigma_{A\pm}^2$ arising from pump-power fluctuations. Thus their total per-mode conditional variances are

$$\sigma_{A\pm}^{\text{tot}2} = F_{\text{APD}}(\sigma_{A\pm}^2 + \sigma_{P\pm}^2) + \sigma_D^2 \quad \text{and} \quad \sigma_{E\pm}^{\text{tot}2} = F_{\text{APD}}\sigma_{A\pm}^2 + \sigma_D^2. \quad (35)$$

IV. PARAMETER VALUES

Table I lists experimentally-determined parameter values for the experiment that yielded the data reported as blue circles and green triangles in the Letter's Fig. 2.

Parameter	Symbol	Value
Alice's fluorescence bandwidth	W	2 THz
Alice's signal transmissivity	κ_A	0.74
Alice-to-Bob transmissivity	κ_1	0.50
Bob's pre-EDFA transmissivity	κ_B	0.43
Bob's BPSK modulation rate	R	500 kbit/s
Bob's BSPK bit duration	T	2 μ s
Bob's EDFA gain	G_B	1.34×10^4
Bob's EDFA per-mode ASE	N_B	1.46×10^4
Bob's post-EDFA transmissivity	κ'_B	0.39
Bob-to-Alice transmissivity	κ_2	0.90
Alice's return transmissivity	κ'_A	0.41
Alice's idler transmissivity	κ_I	0.39
Alice's OPA gain -1	$G_A - 1$	1.86×10^{-5}
Alice's detection efficiency	κ_d	0.45
Alice's modulation-depth efficiency	η_d^A	0.52
Alice's number of mode pairs	M	4×10^6
Eve's return transmissivity	κ_E	0.013
Eve's mixing transmissivity	η_E	0.99
Eve's detection efficiency	κ'_d	0.5
Eve's modulation-depth efficiency	η_d^E	0.17
APD noise figure	F_{APD}	3.0
Electronics-noise variance	σ_D^2	6.0×10^{-3}

TABLE I: Experimentally-determined parameter values for the experiment that yielded the BER data reported in the Letter's Fig. 2.

V. BIT-ERROR RATE FOR GAUSSIAN-DISTRIBUTED OBSERVATIONS

Suppose that we observe a continuous random variable x , whose statistics depend on the discrete random-variable message y that is equally likely to be $+1$ or -1 . In particular, let x be Gaussian distributed with mean value m_+ and variance σ_+^2 when $y = +1$, and let x be Gaussian distributed with mean value m_- and variance σ_-^2 when $y = -1$, where $m_+ > m_-$ and $\sigma_+^2 > \sigma_-^2$. With the appropriate identifications for the conditional means and variances, this setup encompasses both Alice and Eve's receiver statistics.

We will assume that the receiver employs a threshold-test decision rule,

$$\begin{array}{ccc}
 & \text{say } y = +1 \text{ sent} & \\
 x & \begin{array}{c} \geq \\ < \end{array} & \gamma, \\
 & \text{say } y = -1 \text{ sent} &
 \end{array} \tag{36}$$

where the threshold, γ , is chosen to equalize the false-alarm and miss probabilities, i.e.,

$$P_F \equiv \Pr(\text{say } y = +1 \text{ sent} \mid y = -1 \text{ sent}), \tag{37}$$

and

$$P_M \equiv \Pr(\text{say } y = -1 \text{ sent} \mid y = +1 \text{ sent}). \tag{38}$$

The threshold that yields this equality is

$$\gamma = \frac{m_+\sigma_- + m_-\sigma_+}{\sigma_+ + \sigma_-}, \tag{39}$$

which leads to

$$P_F = P_M = Q\left(\frac{m_+ - m_-}{\sigma_+ + \sigma_-}\right). \quad (40)$$

For the bit-error rate we thus get

$$\text{BER} = \Pr(y = +1)P_M + \Pr(y = -1)P_F = Q\left(\frac{m_+ - m_-}{\sigma_+ + \sigma_-}\right). \quad (41)$$

Moreover, because $P_F = P_M$ the binary communication channel whose input is y and whose output is the result of the preceding threshold test is a binary symmetric channel.

VI. ALICE AND EVE'S BIT ERROR RATES

Applying the central limit theorem to the sum of $M \gg 1$ conditionally independent (given Bob's BPSK modulation), identically distributed mode-pair contributions that comprise Alice and Eve measurements leads to a model of the form considered in the preceding section with

$$m_{\pm} \equiv M\bar{m}_A \pm M\zeta_A\sqrt{N_S(N_S+1)}/2 \quad \text{and} \quad \sigma_{\pm}^2 \equiv M\sigma_{A\pm}^{2\text{tot}} \quad (42)$$

for Alice when she uses her SPDC source, and

$$m_{\pm} \equiv M\bar{m}_E \pm M\zeta_EN_S/2 \quad \text{and} \quad \sigma_{\pm}^2 \equiv M\sigma_{E\pm}^{2\text{tot}} \quad (43)$$

for Eve, where the constants \bar{m}_A and \bar{m}_E do not affect the BERs. The Letter's Eqs. (1) and (2) then follow immediately from the preceding BER theory for Gaussian-distributed observations. When Alice uses a source that produces M statistically independent, identically distributed, zero-mean, jointly-Gaussian signal-idler mode pairs whose phase-sensitive cross correlation is at the classical limit for the N_S source brightness, her BER follows from the Gaussian-observation theory but with

$$m_{\pm} \equiv M\bar{m}_A \pm M\zeta_A N_S/2 \quad \text{and} \quad \sigma_{\pm}^2 \equiv M\sigma_{A\pm}^{2\text{tot}}. \quad (44)$$

VII. ALICE'S SHANNON INFORMATION AND EVE'S HOLEVO INFORMATION

Alice's Shannon information (in bits) is given by

$$I_{AB} = \sum_{a,b} \Pr(a,b) \log_2 \left(\frac{\Pr(b|a)}{\Pr(b)} \right), \quad (45)$$

where $b = 0, 1$ and $a = 0, 1$ are the values of Bob's transmitted and Alice's decoded bits. Taking Bob's bit to be equally likely 0 or 1, and using the fact that the Bob-to-Alice channel is binary symmetric—i.e., Alice's false-alarm and miss probabilities both equal the error probability from the Letter's Eq. (1)—we get

$$I_{AB} = 1 - \text{BER}_A \log_2(\text{BER}_A) \quad (46)$$

$$- (1 - \text{BER}_A) \log_2(1 - \text{BER}_A). \quad (47)$$

Eve collects a set of M conditionally independent (given Bob's modulation), identically-distributed mode pairs from the Alice-to-Bob and Bob-to-Alice channels. Denoting the annihilation operators for a generic mode pair from this set by $\{\hat{a}_{E_1}, \hat{a}_{E_2}^{\pm}\}$, we have that each mode pair, given Bob's modulation, is in a zero-mean, jointly-Gaussian state whose density operator $\hat{\rho}_{E_1 E_2}^{\pm}$ is completely characterized by the covariance matrix $\Gamma_{E_1 E_2}^{\pm} \equiv \langle [\hat{a}_{E_1}^{\dagger} \hat{a}_{E_2}^{\pm\dagger} \hat{a}_{E_1} \hat{a}_{E_2}^{\pm}]^T [\hat{a}_{E_1} \hat{a}_{E_2}^{\pm} \hat{a}_{E_1}^{\dagger} \hat{a}_{E_2}^{\pm\dagger}] \rangle$ satisfying

$$\Gamma_{E_1 E_2}^{\pm} = \begin{bmatrix} N_{E_1} & 0 & C_{E_1 E_2}^{\pm} & 0 \\ 0 & N_{E_2} & 0 & C_{E_1 E_2}^{\pm} \\ C_{E_1 E_2}^{\pm} & 0 & N_{E_1} + 1 & 0 \\ 0 & C_{E_1 E_2}^{\pm} & 0 & N_{E_2} + 1 \end{bmatrix}. \quad (48)$$

Here, $N_{E_1} \equiv \langle \hat{a}_{E_1}^\dagger \hat{a}_{E_1} \rangle$, $N_{E_2} \equiv \langle \hat{a}_{E_2}^{\pm\dagger} \hat{a}_{E_2}^\pm \rangle$, and $C_{E_1 E_2}^\pm \equiv \langle \hat{a}_{E_1}^\dagger \hat{a}_{E_2}^\pm \rangle$, where we have exploited the photon-number preserving nature of BSPK modulation and taken the cross-correlation to be real valued. Eve's Holevo information (in bits) is

$$\chi_{EB} = S(\hat{\rho}_{E_1 E_2}) - M[S(\hat{\rho}_{E_1 E_2}^+) + S(\hat{\rho}_{E_1 E_2}^-)]/2, \quad (49)$$

where $\hat{\rho}_{E_1 E_2}$ is Eve's *unconditional* joint state for all M mode pairs, and $S(\hat{\rho})$ is the von Neumann entropy (in bits) of the density operator $\hat{\rho}$. The conditional density operators $\hat{\rho}_{E_1 E_2}^\pm$ are zero-mean, jointly-Gaussian states whose von Neumann entropies are easily evaluated from the symplectic-decomposition technique developed in [18]. Eve's unconditional density operator is *not* Gaussian, but it is zero-mean and its covariance matrix, $\mathbf{\Gamma}_{E_1 E_2}$, is block diagonal with each block equaling

$$(\mathbf{\Gamma}_{E_1 E_2}^+ + \mathbf{\Gamma}_{E_1 E_2}^-)/2 = \quad (50)$$

$$= \begin{bmatrix} N_{E_1} & 0 & 0 & 0 \\ 0 & N_{E_2} & 0 & 0 \\ 0 & 0 & N_{E_1} + 1 & 0 \\ 0 & 0 & 0 & N_{E_2} + 1 \end{bmatrix}. \quad (51)$$

Thus $\mathbf{\Gamma}_{E_1 E_2}$ is identical to the covariance matrix of $2M$ independent thermal states, half with average photon number N_{E_1} and half with average photon number N_{E_2} . So, because a thermal state of average photon number N has the maximum von Neumann entropy of all states with that average photon number, we get the upper bound

$$\chi_{EB} \leq \chi_{EB}^{\text{UB}} \equiv M[g(N_{E_1}) + g(N_{E_2})] - M[S(\hat{\rho}_{E_1 E_2}^+) + S(\hat{\rho}_{E_1 E_2}^-)]/2 \quad (52)$$

on Eve's Holevo information, where $g(N) \equiv (N+1)\log_2(N+1) - N\log_2(N)$ is the von Neumann entropy (in bits) for the thermal state with average photon number N .

VII. NOISE THRESHOLD FOR CLASSICALITY

Alice's returned and retained light are in a classical state when Bob's ASE has per-mode average photon number N_B such that

$$|\langle \hat{a}_{I_1} \hat{a}_{S_8}^\pm \rangle|^2 \leq \langle \hat{a}_{I_1}^\dagger \hat{a}_{I_1} \rangle \langle \hat{a}_{S_8}^{\pm\dagger} \hat{a}_{S_8}^\pm \rangle. \quad (53)$$

Evaluating the moments in this inequality yields

$$\kappa_I \kappa'_A \kappa_2 \kappa'_B G_B \kappa_B \kappa_1 \kappa_A N_S (N_S + 1) \leq \kappa_I N_S (\kappa'_A \kappa_2 \kappa'_B G_B \kappa_B \kappa_1 \kappa_A N_S + \kappa'_A \kappa_2 \kappa'_B N_B), \quad (54)$$

which simplifies to

$$N_B \geq N_B^{\text{thresh}} \equiv \kappa_1 \kappa_A \kappa_B G_B. \quad (55)$$